日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年　５月２３日

出 願 番 号
Application Number: 特願２０００－１５５９５４

出 願 人
Applicant (s): 株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１０月　６日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号　出証特２０００－３０８１６８４

【書類名】　特許願

【整理番号】　H00009231A

【提出日】　平成12年 5月23日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 15/16

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内

【氏名】　小原　清弘

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【電話番号】　03-3212-1111

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　計算機システムおよびデータ復号化方法

【特許請求の範囲】

【請求項１】

第二の計算機システムと通信路で接続されている第一の計算機システムであって、

前記第一の計算機システムは、前記第二の計算機システムから暗号化データを受け取り、当該暗号化データを復号化せずに格納することを特徴とする計算機システム。

【請求項２】

第二の計算機システムと通信路で接続されている第一の計算機システムであって、

前記第一の計算機システムはストレージシステムを有し、前記第二の計算機システムから暗号化データを受け取り、当該暗号化データを復号化せずに前記ストレージシステムに格納することを特徴とする計算機システム。

【請求項３】

前記第一の計算機システムはネットワーク接続装置を有し、前記第二の計算機システムから暗号キーと暗号化データを受け取り、当該暗号化データを復号化せずに前記ストレージシステムに格納することを特徴とする請求項２記載の計算機システム。

【請求項４】

前記第一の計算機システムはプロセッサシステムを有し、前記第二の計算機システムから暗号キーと暗号化データを受け取り、当該暗号化データを復号化せずに前記ストレージシステムに格納することを特徴とする請求項２または３記載の計算機システム。

【請求項５】

前記プロセッサシステムは、前記ストレージシステムから暗号化データを読み出し、復号化し、さらに前記ストレージシステムに書き込むことを特徴とする請求項２乃至４記載の計算機システム。

【請求項６】

前記ネットワーク接続装置は、前記ストレージシステムから暗号化データを読み出し、復号化し、さらに前記ストレージシステムに書き込むことを特徴とする請求項２乃至５記載の計算機システム。

【請求項７】

前記ストレージシステムが、当該ストレージシステム自身内の暗号化データを読み出し、復号化し、書き込むことを特徴とする請求項２乃至４に記載の計算機システム。

【請求項８】

前記第一の計算機システムは復号化装置を有し、前記復号化装置は前記ストレージシステムから暗号化データを読み出し、復号化し、さらに前記ストレージシステムに書き込むことを特徴とする請求項２乃至４に記載の計算機システム。

【請求項９】

前記ストレージシステムからの暗号化データの読み出しと復号化データの書き込みが、当該ストレージシステムにおける同一の記憶位置に対して実行されることを特徴とする請求項５乃至８に記載の計算機システム。

【請求項１０】

前記ストレージシステム中に、受け取った暗号化データを復号化せずに、受け取った順番で格納し、当該ストレージシステムからの暗号化データの読み出しと復号化データの書き込みが、該ストレージシステムの読み出された位置と異なる位置に書き込むことを特徴とする請求項５乃至８に記載の計算機システム。

【請求項１１】

前記第一の計算機システム内における暗号化データの読み出し間隔が、一定時間間隔であることを特徴とする請求項５乃至１０記載の計算機システム。

【請求項１２】

前記第一の計算機システム内における暗号化データの読み出しが、前記第一の計算機システム内のストレージシステムからの要求により起動されることを特徴とする請求項５乃至１１に記載の計算機システム。

【請求項１３】

前記第一の計算機システム内のストレージシステムから暗号化キーを受け取ることを特徴とする請求項５乃至１２に記載の計算機システム。

【請求項１４】

前記第一の計算機システム内のネットワーク接続装置から暗号化キーを受け取ることを特徴とする請求項５乃至１２に記載の計算機システム。

【請求項１５】

前記第一の計算機システム内のプロセッサシステムから暗号化キーを受け取ることを特徴とする請求項５乃至１２に記載の計算機システム。

【請求項１６】

計算機システム内で受け取った暗号化データを復号化せずに格納するストレージシステムから暗号化データを読み出して復号化し、さらに前記ストレージシステムに書き込むことを特徴とする暗号化復号方法。

【請求項１７】

計算機システム内で受け取った暗号キーと暗号化データを復号化せずに格納するストレージシステムから暗号キーを復号化装置へ渡し、受け取った前記暗号化データを順次前記復号化装置へ送り復号化し、さらに前記復号化装置から前記ストレージシステムに書き込むことを特徴とする暗号化復号方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はリモートコピー（遠隔データバックアップとも呼ばれる）による、情報処理システムのデータ保存に関する。特にローカルシステムとリモートシステム間での、データ暗号化および復号化の方法およびそれを実現するシステムに関する。

【０００２】

【従来の技術】

データバックアップ手法は、計算機システムの障害時において、データの保全および回復を行う重要な手段である。個々の事業所で実際に実施されるバックア

ップ手法は、対処可能な障害の程度、バックアップ先とのデータ差異、適用業務の中断、ストレージシステムの応答時間の遅延の大小などいくつかのパラメタを基準に選択される。

【０００３】

これらバックアップ手法の中で、リモートコピーと呼ばれるバックアップ手法がある。これは、書き込み要求を受けた情報を、ストレージシステム自体が他のストレージシステムへコピーするバックアップ手法である。ここで、コピー元のシステムをローカルシステム、コピー先のシステムをリモートシステムと呼ぶ。リモートコピーの例は、例えば日経ＢＰ社「出揃った並列汎用機とディスク・アレイ」1995/11出版ISBN:482221558Xの、256ページ以降に、SYMMETRIXリモートデータ機能として説明されている。

【０００４】

ここでローカルシステムとリモートシステムを結ぶパスは、近距離の場合はESCON(エンタプライズシステム接続)等のストレージ用インタフェースで可能だが、遠距離の場合は、ディレクタやスイッチを用いた回線経由になる。このような回線、特に公衆回線を経由した場合、データ漏洩対策として、リモートコピーデータの暗号化が頻繁に用いられる。このような暗号化及び復号化は、ストレージシステム自体、又はディレクタやスイッチ等が行う。

【０００５】

【発明が解決しようとする課題】

データ暗号化/復号化は時間のかかる処理である。このため、企業のバックアップセンタやデータセンタ等、複数のシステムから同時に多数の暗号化データを受け取るシステムでは、データの復号化処理がネックとなる。これにより、同時に受け付け可能なデータ量が少なくなり、企業のデータバックアップ量やデータセンタのデータ処理量が制限される事態が生じている。

【０００６】

本発明の目的は、リモートコピー等により暗号化データを受け取るリモートシステムに対し、同時に多数の暗号化データを受け取る手段を提供する事にある。

【０００７】

【課題を解決するための手段】

上記目的は、暗号化データをストレージシステムに書き込む手段、ストレージシステム内のデータが、暗号文か平文かを識別する手段、暗号化データのストレージへの書き込みとは非同期にストレージ内の暗号化データを読み出し復号化し再び書き込む手段により達成される。

【０００８】

【発明の実施の形態】

次に図１～図１４を用いて本発明の第一の実施例を説明する。最初に本発明の主要な適用先である既存のリモートコピー方式の説明を行い、その後で本発明の実施例を説明する。

【０００９】

図２に単一ディスク制御装置の一構成例を示す。ディスク制御装置７は、ホストインタフェース２とチャネルパス８によりホストコンピュータ１と接続し、キャッシュメモリ３、共有メモリ１５、ディスク駆動装置５と接続するディスクインタフェース４およびこれらを接続する共通バス６により構成されている。複数のディスクインタフェースが実装可能である。複数のホストインタフェース２も実装可能であり、この場合接続先のホスト１が同一であるか否かは問わない。本実施例の図２では、各ホストインタフェースが同じホストに接続されている例を示している。

【００１０】

ホストインタフェース２とディスクインタフェース４には、プロセッサが装備されており、それぞれ自律的に動作する。またキャッシュメモリ３、共有メモリ１５、ＬＡＮインタフェース１１は、複数のホストインタフェース２や複数のディスクインタフェース４から参照可能な共有資源である。キャッシュメモリ３には、本ディスク制御装置へ書き込まれたデータやディスク駆動装置５から読み出されホストに出力したデータが一時的に保存される。

【００１１】

ディスク制御装置がディスクアレイ機能を持っている場合には、ホストから送

られたデータは分割され、複数のディスク駆動装置５に分散して格納される。本実施例はディスクアレイに対しても適用可能であるが、説明の簡略化のため、以後の説明は通常のディスク駆動装置に対する動作を例に説明する。

【００１２】

ホストコンピュータ１は、プロセッサ１３、主記憶１２及びI/0制御プロセッサ３８を持つ。I/0制御プロセッサ３８は、ディスク制御装置７との入出力を行う。プロセッサ１３からの指示に基づき、読み出しコマンドの場合は、指定したディスクドライブ（ボリウム）に対する読み出しコマンドを生成し、ディスク制御装置７に送信し、ディスク制御装置７からのデータを受け取り主記憶１２に格納する。書き込みコマンドの場合は、指定したディスクドライブ（ボリウム）に対する書き込みコマンドを生成し、書き込みデータと共にディスク制御装置７に送信する。

【００１３】

図３を用いてリモートコピーシステムの一構成例を示す。リモートコピーは、ディスク制御装置が自律的に、指定されたボリウムを他のディスク制御装置にコピーする機能である。この機能は、ホストインタフェース上のプログラムにより実現される。

【００１４】

ここでは、ローカルシステム９のディスク駆動装置５ａ中のボリウムＡを、リモートシステム１０のディスク駆動装置５ｂ中へコピーしている。図３では、ローカルシステムとリモートシステムが同一の構成のように見えるが、リモートコピーでは、ローカルシステムとリモートシステムが、稼働しているソフトウエアも含め同一構成システムである必要はない。さらに言えば、ここでは便宜的にローカルシステム／リモートシステムと呼んでいるが、一方が他方の待機系である必要もない。例えばローカルシステムが基幹業務システムであり、リモートシステムがデータウエアハウスシステムでも良い。図３においても、ボリウムＡ以外のボリウムは、異なるアプリケーションが利用している異なる内容のボリウムを仮定している。

【００１５】

リモートコピーの動作は、次のようになる。まず、ホスト１ａからのディスクへの書込要求コマンドに対し、ホストインタフェース＃０（２ａ）は、その書込先のボリウムがリモートコピーの対象になっているか否かを判断する。リモートコピー対象ボリウムの情報は、共有メモリ上に置かれており、ホストインタフェース＃０（２ａ）上のプロセッサが共有メモリを参照して判断する。リモートコピーの対象になっていない場合は、そのまま書込要求コマンドを処理する。

【００１６】

書込先がリモートコピーの対象になっている場合は、通常通りに書込要求コマンドを処理すると共に、リモートシステム１０のディスク制御装置７ｂと接続されているホストインタフェース＃１（２ｂ）を使用して、ホストから受け取ったコマンドと同一の書込要求コマンドをディスク制御装置７ｂに発行する。これにより、リモートシステム１０のディスク駆動装置５ｂ上に、ボリウムＡの複製が生成される。これらホストインタフェース２は、入出力コマンドの発行処理と受信処理の両方の機能を備えている。これらコマンドの処理/生成機能はホストインタフェース２中のプロセッサの処理により実現される。

【００１７】

リモートコピーの開始／終了等は、通常の入出力命令と同様なコマンドを用いホスト上のプログラムから制御される。主なコマンドを次に述べる。

【００１８】

(1) 初期化&コピー開始コマンド（コピー先のボリウムの内容をコピー元と同一にするために指定されたボリウムの全内容をコピー先へコピーする（初期化）と共に、ホストから発行された書込要求コマンドに対し、指定されたコピーモード（同期／非同期）でリモートコピーを開始する）

(2) 中断コマンド（リモートコピーを一時中断する。この後に受け付けた書込要求コマンドに対するリモートコピーデータはバッファに保存しておき、後の再開コマンドに備える）

(3) 再開コマンド（中断していたリモートコピーを再開する。バッファに保存されているリモートコピーデータに対してもコピーを行う）

(3) フラッシュコマンド（バッファに保存されているリモートコピーデータを強制的にコピー先へコピーする）

図３では、ローカルシステムとリモートシステム間は、ホストコンピュータとストレージシステムを接続するチャネルパスと同じ種類のパスで結ばれている。しかし一般的なチャネルパスの物理/電気的仕様は、比較的短距離間の接続を前提にしている。

【００１９】

例えばＳＣＳＩ－２（スモール・コンピュータ・システム・インタフェース－２）規格（ANSI X3.131-1994）として知られるディスク及び周辺機器インタフェースでは、接続距離は最大２５ｍ。光接続を用いるインタフェースでも、ファイバチャネル規格（ANSI X3.230-1994）が最大１０ｋｍ、ＥＳＣＯＮ規格が最大６０ｋｍである。したがってこのようなチャネルパスは、災害対策等の目的で行われるリモートコピーにおいて、遠距離、例えば東京－大阪間、のローカル－リモートシステム間を結合する方式には適さない。

【００２０】

チャネルパスの結合距離を長距離に伸ばすには、図４に示すように、ＮＴＴ等の通信事業者が提供するＷＡＮ（ワイド・エリア・ネットワーク）２４を利用するのが一般的である。この場合ＷＡＮ２４との接続点に、ディレクタ２２やエクステンダ、又はスイッチ等の変換装置を設置する構成になる。

【００２１】

このような変換装置には、例えば米国ＣＮＴ社の、ＵＬＴＲＡＮＥＴ　ＳＴＯＲＡＧＥ　ＤＩＲＥＣＴＯＲがある。このディレクタ２３はＷＡＮ２４を挟んでもう一つのディレクタ２４と対になって用い、チャネルパス８ａ上のプロトコルとＷＡＮ２４上のプロトコルの相互変換を行う。これにより、チャネルパス８ａ上のデータを、ＷＡＮ２４を経由して、相手側のチャネルパス８ｂ上に伝達できる。

【００２２】

これら変換は独立して行われるため、チャネルパス８ａや８ｂを使用するストレージシステム７ａ、７ｂやホストコンピュータ１ａ、１ｂでは、ＷＡＮ２４を

経由している事は認識されず、通常のチャネルパス接続と等価に見える。このため、ストレージシステムやホストコンピュータ上のプログラムを変更すること無しに、遠距離間のデータ入出力が可能になる。

【００２３】

このような変換装置には、例えば米国ＣＮＴ社の、ＵＬＴＲＡＮＥＴ　ＳＴＯＲＡＧＥ　ＤＩＲＥＣＴＯＲがある。このディレクタ２３はＷＡＮ２４を挟んでもう一つのディレクタ２４と対になって用い、チャネルパス８ａ上のデータを、ＷＡＮ２４を経由して、相手側のチャネルパス８ｂ上に伝達する。チャネルパス８ａや８ｂを使用するストレージシステム７ａ、７ｂやホストコンピュータ１ａ、１ｂでは、ＷＡＮ２４を経由している事は認識されず、通常のチャネルパス接続と等価に見える。このため、ストレージシステムやホストコンピュータ上のプログラムを変更すること無しに、遠距離間のデータ入出力が可能になる。

【００２４】

このようにＷＡＮを経由してデータの交換を行う場合、データの機密性を保つため、データの暗号化を行う。暗号化及び復号化を行う主体はいくつかのケースが考えられるが、ここではストレージシステムが暗号化するケースについて説明する。図５にストレージシステムのホストインタフェース２で暗号化/復号化を行う場合の、ホストインタフェース２の内部構成例を示す。

【００２５】

ホストインタフェース２は、プロセッサ１６、ローカルメモリ１７、外部インタフェース（外部I/F）１８、アクセス制御部１９、バスインタフェース（バスI/F）２０、暗号化プロセッサ２１により構成される。

【００２６】

チャネルパス８を経由してホストから与えられたコマンドは、外部I/F１８により受信され、アクセス制御部を経由して、プロセッサ１６が受け取る。プロセッサ１６はコマンドの内容を判断し、書き込みコマンドの場合は、バスI/F２０、バス６を経由して、ディスク及びキャッシュに書き込む。データが暗号化されており、復号化の必要がある場合は、暗号化プロセッサを用い復号化したデータを書き込む。

【００２７】

読み出しコマンドの場合も同様に、ディスク又はキャッシュの内容を、バスI/F２０、バス６を経由して読み出し、アクセス制御部１９、外部I/F１８を経由してホストに送信する。データを暗号化する場合は、暗号化プロセッサを用いデータを暗号化した後に送信する。

【００２８】

このように、ストレージシステムでの暗号化及び復号化は、データの送受信時に行われるのが一般的である。これに対し、本発明による暗号化データのリモートコピーの、データ受信方式を図１に示す。この方式は、図４で説明したリモートシステム１０に対し適用する方式である。

【００２９】

本方式でのストレージシステムのハードウエア構成は、図２、図４および図５で説明した従来のシステムと基本的に同等である。ストレージシステム中の暗号化プロセッサは不要である。本方式では、復号化処理をデータ受信とは非同期に行い、また復号化する主体もストレージシステムではなく、ホストが実行するところに特徴がある。

【００３０】

本方式でのリモートコピーデータの受信及び復号化の手順を、図６から図８のフローチャートを用いて説明する。

【００３１】

リモートコピーデータの受信処理のフローチャートを図６に示す。この処理は、ホストインタフェース＃２（２ｃ）が行う処理である。ここではこのホストインタフェースは、暗号化されたリモートコピーデータの受信専用に利用されているため、本フローチャートではデータ部分が暗号化された書き込みコマンドに対する処理手順を示す。

【００３２】

コマンド待ち（１００）中に、暗号化された書き込みを受信すると、ホストインタフェース＃２（２ｃ）は、書き込みコマンドで指定されたディスク(ボリウム)に対して、そのコマンドで指定された位置へデータを書き込み（１０１）、

その書き込みデータの情報を、共有メモリ上に格納されている暗号化データテーブルに登録（１０２）する。

【００３３】

暗号化された書き込みコマンドのフォーマット例を図９に示す。チャネルパス８ｂ上のコマンドが、ＳＣＳＩ－２コマンドの場合を示している。ＬＵＮ２７は、ロジカルユニット番号のフィールドであり、書き込み先のディスク（ボリウム）を指定する。論理ブロック・アドレス２８は、データの書き込みを開始する位置を示す。書き込みデータの長さは、書き込みデータ長２９で示される。書き込みデータ３０自体は暗号化され、１０バイト目以降に付けられている。その他のフィールドは、本発明では利用しないので説明を省略する。

【００３４】

図１０は暗号化される前のコマンドフォーマットである。図９との対比で判るとおり、暗号化が施されているのはデータ部分だけである。このため、データを受け取るホストインタフェース＃２（２ｃ）は復号化処理を行わないで、指定されたディスク上の位置へデータを書き込める。

【００３５】

暗号化後のデータの長さは、暗号化前のデータの長さと同じと仮定している。このような仮定は、例えばＤＥＳ（データ・エンプリクション・スタンダード）の暗号化方式では成立する。コマンド全てが暗号化されている場合や暗号化後にデータ長が変わる暗号化方式を採用した場合の処理手順は、第二の実施例で示す。

【００３６】

図１１に暗号化テーブルの構成例を示す。このテーブルはロジカルユニット番号３５、論理ブロックアドレス３６、書き込みデータ長３７の各フィールドからなる。このフィールドの意味は、書き込みコマンドの同一名のフィールドと同じである。このテーブルのデータを参照することにより、暗号化されたた書き込まれたデータの位置を知ることが出来る。例えば最初のエントリは、ロジカルユニット番号０番のディスク（ボリウム）の、論理ブロックアドレス１０番から１００ブロックの長さのデータが暗号化されている事を示す。ロジカルユニット番号

が－１のエントリは、最終エントリ、すなわち暗号化テーブルの終わりを示す。

【００３７】

本方式では処理時間のかかる復号化処理を受信時に実行しない。このためデータ受信のスループットを向上することができる。これは特に複数の相手からの暗号化データを受信する場合に効果的である。

【００３８】

このように暗号化したままの保存は、いくつかの場面で非常に有効である。例えば、リモートシステムで万が一データが盗難や流出したとしても、暗号化キーも同時に持ち出されない限り安全である。すなわち、暗号化キーをリモートシステムに渡さなければ、上記のような盗難や流出に対する安全性が確保される。リモートコピー先をデータ保管金庫として利用する場合は、このような方法が適している。

【００３９】

一方、災害対策としてのリモートコピーを考えた場合、ローカルシステムがダウンした後には、コピーされたデータ及びリモートシステムを用いて出来るだけ早く業務を再開する必要がある。このためには、業務再開時にはコピーされたデータが平文に戻っている必要がある。本発明では、この復号化をリモートシステムのホストコンピュータが実行する。

【００４０】

復号化処理のフローチャートを図７に示す。この処理は、ホストコンピュータ（１ｂ）上の復号化プログラム２５が行う処理である。最初に、ディスク制御装置内の暗号化テーブルを読み出す（１１０）。ホストコンピュータ（１ｂ）は、このテーブルを参照することにより、復号化が必要なデータの位置を得る。

【００４１】

続いて、読み出した暗号化テーブルのエントリの情報を参照し、復号化が必要なデータをディスクシステムから読み出し（１１１～１１２）、復号化処理を行い（１１３）、ディスクシステム上の同じ位置へ書き戻す（１１４）。これらの復号化を、暗号化テーブルの全てのエントリに対して繰り返す（１１５、１１１、１１６）。この一連の処理により、ディスク上の暗号化データが平文に復号化

される。

【００４２】

本実施例では、暗号化テーブルはディスクシステムの共有メモリ上に格納される。したがってホストコンピュータ（１ｂ）が暗号化テーブルを読み出すには、専用の読み出しコマンドを使用する。この専用コマンドは、例えばＳＣＳＩ－２コマンド体系の場合、コマンドの最初の８ビットを、規格で使用されていない値とすることで実現する。

【００４３】

この暗号化テーブル読み出しコマンドは、ホストコンピュータ（１ｂ）のI/O制御プロセッサ３８により生成され、ディスク制御装置７ｂのホストインタフェース＃３（２ｄ）により解釈される。すなわちホストインタフェース＃３（２ｄ）は通常の読み出しや書き込みコマンドの他に、暗号化テーブル読み出しコマンドを処理する。この処理を実現するための、ホストインタフェース＃３（２ｄ）の手順を、図８のフローチャートに示す。

【００４４】

ホストインタフェース＃３（２ｄ）は、コマンド受信（１２０）後、そのコマンドが暗号化テーブル読み出しコマンドかをチェックする（１２１）。暗号化テーブル読み出しコマンド以外の場合は、通常のコマンド処理を行う（１２６）。

【００４５】

暗号化テーブル読み出しコマンドの場合は、最初に共有メモリ上の暗号化テーブルをロックする（１２２）。このロックにより、ホストインタフェース＃３（２ｄ）が暗号化テーブルを読み出し中に、暗号化されたリモートコピーのデータを受け付けた他ホストインタフェースが暗号化テーブルを更新し、不完全なデータをホストに送信するのを防ぐ。したがってこのロックが有効な間は、図６のフローチャートで説明した暗号化テーブルの更新処理は保留される。

【００４６】

ロックが完了した後、暗号化テーブルの内容を読み出し（１２３）、ホストに送信する（１２４）。続いて暗号化テーブルを初期化する（１２５）。初期化の理由は、ホストに送信した暗号化テーブルの内容が示す領域は必ず復号化される

ので、この情報を保持する必要が無くなるためである。最後に暗号化テーブルのロックを解除し（１２５）、新たに受け入れた暗号化データの位置を記憶できるようし、一連の処理を終了する。

【００４７】

リモートシステムに存在するホストが暗号化データを復号化するには、ローカルシステムから暗号化キーを受け取る必要がある。この暗号化キーの交換は、リモートコピーの開始時に行う。具体的には、図４において、ホスト１ａからローカルシステムのディスク制御装置７ａに、リモートコピーの「初期化＆コピー開始コマンド」が発行された時、ローカルのディスク制御装置７ａから、リモートのディスク制御装置７ｂに暗号化キーが渡され、その後データのコピーが開始される。さらに、リモートホスト１ｂが復号化のため暗号化テーブル読み出しコマンドを発行した時、ディスク制御装置７ｂから暗号化テーブルと共に暗号化キーがホストコンピュータ１ｂに渡される。

【００４８】

このような暗号化キーの交換は、暗号化方式が公開鍵方式の場合は不要である。しかし公開鍵方式は秘密鍵方式と比較して、暗号化速度が非常に遅いという欠点がある。一方、秘密鍵をそのままWANを経由して送信するのも機密上問題がある。このため、リモートコピーデータの暗号化は秘密鍵方式で行い、前述した暗号化キーの交換だけ、公開鍵方式で暗号化キーを暗号化して渡す方式が効率的である。

【００４９】

また本発明のディスク制御装置は、LANインタフェースを具備している。したがって、LANを経由してローカルのディスク制御装置７ａと、リモートのホスト１ｂが直接暗号化キーを授受することも可能である。この場合も、暗号化キーがそのままLAN上に送出するのは機密性に問題がある。したがってこの場合、公知の技術であるHTTPSやIPsec等、LAN上で機密を保ったまま通信を行うプロトコルを使用して送信する。

【００５０】

図７で示した、ホストが行う復号化を実行するタイミングは、複数の実施形態

がある。一つは一定時間間隔で実行する方法である。すなわちホスト上の復号化プログラム２５が一定時間間隔で暗号化テーブルを読み出し、その内容に沿って復号化する。

【００５１】

大量に暗号化リモートコピーデータを受け付けた場合、共有メモリ上の暗号化テーブルの領域が不足する場合がある。このような場合、ディスク制御装置７ｂ側からホスト上の復号化プログラム２５に対して通知を行い、復号化処理を起動させる。

【００５２】

具体的には、ホストインタフェース＃２（２ｃ）からホストインタフェース＃３（２ｄ）に通知し、ホストインタフェース＃３（２ｄ）が復号化処理起動コマンドをホストコンピュータ１ｂ送信する。復号化処理起動用のコマンドを受け取ったホストコンピュータ１ｂのI/O制御プロセッサ３８は、復号化プログラム２５に対し通知を行い復号化処理を起動する。復号化起動コマンドは、暗号化テーブル読み出しコマンドと同様に、未定義のコマンドを流用する。

【００５３】

またホストコンピュータ１ｂとディスク制御装置７ｂはＬＡＮで接続されている。したがってＬＡＮインタフェースを使用して、ＬＡＮ経由で復号化処理の起動を通知することもできる。

【００５４】

ここまでの実施例では、暗号化テーブルはディスク制御装置７ｂ内の共有メモリ１５上に置かれているとして説明した。しかし暗号化テーブルの格納場所はこれに限定されない。例えば、ディスク制御装置が管理する特定のディスク（ボリウム）上に置いても、本発明の目的は達せられる。この場合、ホストコンピュータ１ｂによる暗号化テーブルを読み出しは、通常のディスクの読み出しコマンドで実行できる。

【００５５】

さらには、復号化を行う主体に関しても、ホストコンピュータ１ｂに限定されない。本発明では、暗号化テーブルを使用することにより、暗号化データの受信

処理から復号化処理開始までの時間間隔を任意にし、各処理を非同期に実行可能なシステムを提示している。したがって復号化する主体が、ホストインタフェースの場合や、ディスク制御装置７ｂ内の共通バス６に接続された復号化装置等の場合でも同様に適用可能である。

【００５６】

また図１４に示すように、ホスト自身がリモートコピーデータを受け取る場合にも適用できる。この場合、ホストは暗号データを受信し、復号化せずにディスクシステムに書き込み、その後ディスクシステムから暗号化データを読み出し、復号化した後に再び書き込む。

【００５７】

さらにこれら実施形態全てに対し、復号化処理は、ソフトウエアだけではなく復号化ハードウエア又はハードウエアとソフトウエアの組み合わせでも同様の効果を得られる。

【００５８】

本発明の第二の実施例を説明する。

【００５９】

本実施例では、リモートコピーデータが、データ部分だけでなく、ロジカルユニット番号等、コマンドパラメタも含め全ての部分が暗号化された場合を説明する。すなわち図９の全てのフィールドが暗号化された場合である。暗号化がディスク制御装置の外で行われた場合も、コマンドパラメタとデータ部分の切り分けが困難なため、同様の状態となる。より詳細に言えば、図４において、チャネルパス８ａ以降で暗号化された場合である。

【００６０】

これ以降、図１２に示すように、ローカルシステム９のディレクタとＷＡＮの入口の間で暗号化された場合を例にして説明する。

【００６１】

この構成では、全ての部分が暗号化されたパケットが、ディスク制御装置７ｃのホストインタフェース＃２（２ｃ）に届く。ホストインタフェース＃２（２ｃ）は、受け取ったパケットをそのまま復号化しないで、ログボリウム４０に順番

に格納する。処理時間のかかる復号化を行わないで書き込むことにより、受信のスループットを向上することができる。また、このようにログボリウム４０に格納することにより、本来の格納位置が復号化されるまで不明なデータを一時保存できる。

【００６２】

ログボリウム４０のフォーマットを図１５に示す。ログボリウムは、書き込みデータ長４６と書き込みデータ４７を組として、シーケンシャルな形式でデータを受け取った順番に格納されている。

【００６３】

ホストコンピュータ（１ｂ）上の復号化プログラム２５は、任意のタイミングでログボリウム４０を読み出す。第一の実施例と異なり、ログボリウムは通常のボリウムと同じため、復号化プログラム２５は通常の読み出しコマンドで読み出す。

【００６４】

復号化プログラム２５により読み出された暗号化されたパケットは、ホスト上で復号化され、コマンドパラメータ及びデータが平文になる。ここで、データをコマンドパラメタで指定されたディスク上の位置へ書き込む。これら一連の処理により、暗号化されたデータが、復号化され、目的のディスク上の位置へ格納される。

【００６５】

このようにログを使用する方法は、第一の実施例の説明でも述べたが、データの長さが変化する暗号化方式を使用し、目的のディスク上に位置に暗号化データを書き込めない場合にも使用する。

【００６６】

ホストが行う復号化を実行するタイミングは、第一の実施例と同様に、一定時間間隔で実行する方法、ディスク制御装置７ｂ側からホスト上の復号化プログラム２５に対して通知を行う方法、ＬＡＮインタフェースを使用して通知する方法のいずれも適用可能である。

【００６７】

また復号化を行う主体に関しても、第一の実施例と同様に、ホストコンピュータ１ｂに限定されず、ホストインタフェースや、ディスク制御装置７ｂ内の共通バス６に接続された復号化装置、復号化ハードウエア、ハードウエアとソフトウエアの組み合わせ等が利用可能である。

【００６８】

ここまでの説明では、全ての部分が暗号化されたパケットを、ホストインタフェース＃２（２ｃ）がログボリウム４０に書き込む例を説明した。しかし、ディレクタ２３がログボリウムに書き込むコマンドを発行する構成でも同様の効果を得られる。この場合、ディレクタ２３は単にプロトコルを変換するだけでなく、任意のデータの書き込みコマンドを生成する機能を持つ。

【００６９】

図１３にディレクタ２３の内部構成例を示す。ディレクタ２３は、プロセッサ４１、ローカルメモリ４２、ＷＡＮインタフェース４３、チャネルパスインタフェース４４を備える。ＷＡＮインタフェースから受け取ったパケットは、プロセッサ２３によりプロトコル変換を施され、チャネルパスインタフェースにより４４によりチャネルパス８に送られる。前記の「任意のデータの書き込みコマンド」の生成機能はディレクタ２３上のプロセッサ及びソフトウエアで実現する。

【００７０】

次に暗号化キーの交換について説明する。図１２に示したような暗号化装置３９は、暗号化－復号化の対で使用されるのが一般的である。この対になった装置間で暗号化キーの交換及びデータの暗号化が行われ、機密を保った通信が可能になる。

【００７１】

本発明では、暗号化装置３９を対では使わない。このため、リモートシステムは、ローカルシステムの暗号化装置３９の暗号化キーの交換手順に応答可能な機能を持つ。この機能をＶＰＮ（バーチャル・プライベート・ネットワーク）による暗号化を例に説明する。

【００７２】

ＶＰＮは、ＩＰｓｅｃと呼ばれる技術で実現されている。ＩＰｓｅｃは、国際機関であるＩＥＴＦ（インタネット・エンジニアリング・タスク・フォース）で制定された、ＲＣＦ１８２５規格からＲＣＦ１８２９規格及びＲＣＦ２４０１規格からＲＣＦ２４１２規格で規定されている。

【００７３】

これらの規格により、暗号化キー交換プロトコルＩＫＥ（インタネット・キー・エクスチェンジ）が規定されている。このためリモートシステム側で、ＩＫＥに対応する処理を行う事により、図１２のシステム構成での暗号化キーを交換を実現する。ＩＫＥは、ＷＡＮ上のプロトコルの一つである、ＩＰ（インタネット・プロトコル）パケットに対する処理規格である。このため本発明では、ＷＡＮに接続されているディレクタ２３がＩＫＥ処理を行うことにより、暗号化キーを入手し復号化を可能にする。ディレクタ２３は、図１３に示すようにプロセッサを持っており、具体的にはこのプロセッサがＬＡＮインタフェースが受信したＩＰパケットを処理することで、ＩＫＥ処理を実現する。

【００７４】

ディレクタ２３が受け取った暗号化キーは、第一の実施例でも使用したように、ＳＣＳＩ－２の未使用コマンドを利用してディスク制御装置７ｂに渡す。さらに第一の実施例と同様に、ホストコンピュータ１ｂに渡す。これら暗号化キーの渡し方も、第一の実施例と同様に、ＬＡＮ経由が可能である。

【００７５】

以上の手順により、本発明の目的である、リモートコピー等により暗号化データを受け取るリモートシステムに対し、同時に多数の暗号化データを受け取る手段が達成される。

【００７６】

以上第一および第二の実施例では説明の簡略化のため、ローカルシステムとリモートシステムが一対一の構成で説明した。しかし本発明は、多対一、すなわち複数のローカルシステムから同時にデータを受け取るリモートシステムに適用した場合により効果を発揮する。

【００７７】

さらに、第一および第二の実施例ではリモートコピーを例に説明したが、一般的なクライアントーサーバ構成にも適用できる。この場合、ローカルシステムがクライアント、リモートシステムがサーバに対応する。

【００７８】

【発明の効果】

本発明によれば、暗号化データを受け取るシステム対し、時間のかかるデータ復号化の処理を非同期に実行でき、同時に多数の暗号化データを受け取ることが可能になる。

【図面の簡単な説明】

【図１】

リモートコピーされた暗号化データの受信方式の一構成例を示す図である。

【図２】

単一ディスク制御装置の一構成例を示す図である。

【図３】

リモートコピーシステムの一構成例を示す図である。

【図４】

ＷＡＮを使用したリモートコピーシステムの一構成例を示す図である。

【図５】

ホストインタフェースの内部構成の一例を示す図である。

【図６】

リモートコピーデータの受信処理のフローチャートを示す図である。

【図７】

復号化処理のフローチャートを示す図である。

【図８】

ホストインタフェースの処理手順を示すフローチャートを示す図である。

【図９】

暗号化された書き込みコマンドのフォーマットの一例を示す図である。

【図１０】

暗号化される前の書き込みコマンドのフォーマットの一例を示す図である。

【図１１】

暗号化テーブルの構成の一例を示す図である。

【図１２】

ＷＡＮの入口の間で暗号化されたリモートコピーシステムの一構成例を示す図である。

【図１３】

ディレクタの内部構成の一例を示す図である。

【図１４】

ＷＡＮを使用したリモートコピーシステムのもう一つの構成例を示す図である。

【図１５】

ログボリウムのフォーマットの構成例を示す図である。

【符号の説明】

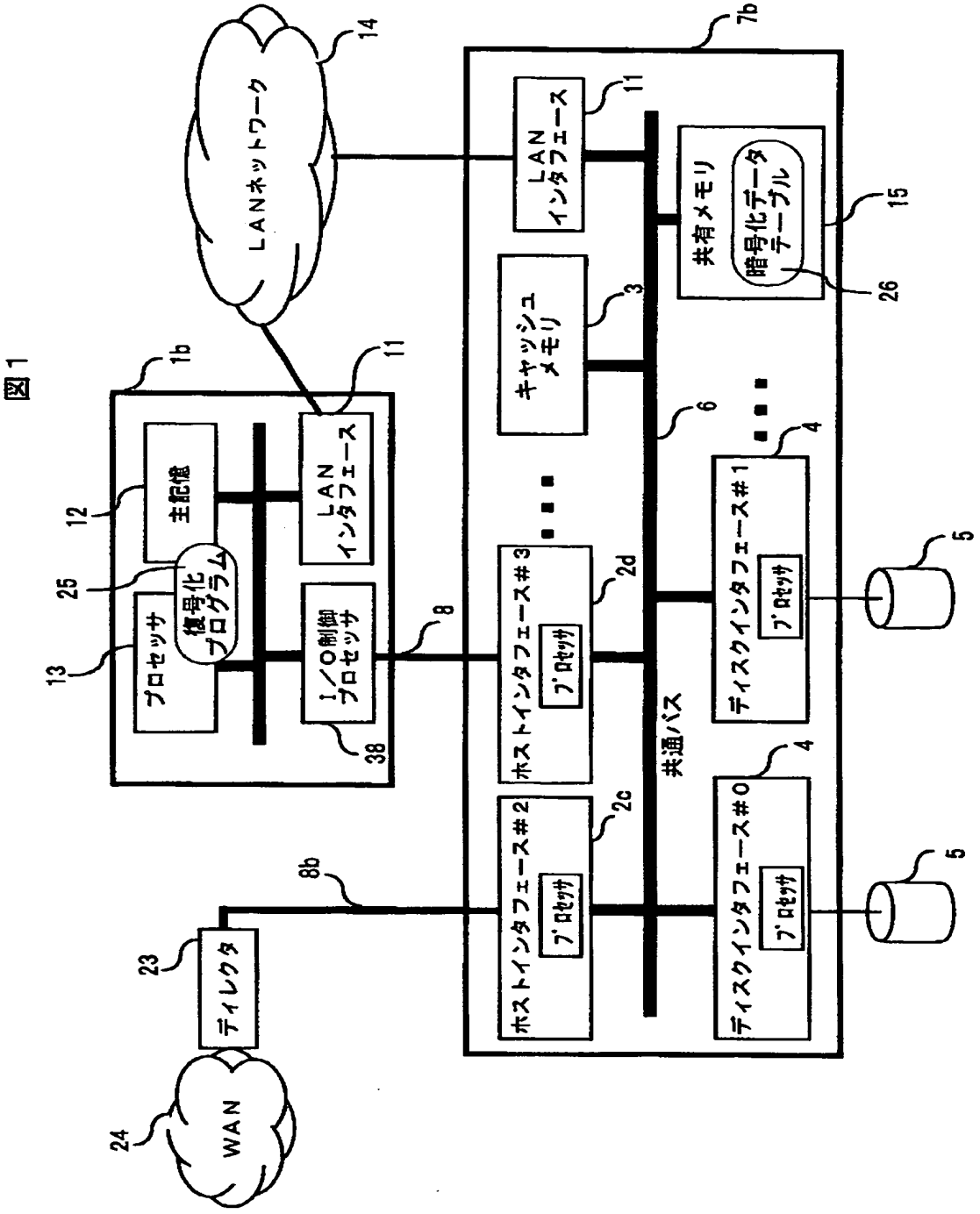
１、１ａ、１ｂ……ホストコンピュータ、２……ホストインタフェース、３……キャッシュメモリ、４……ディスクインタフェース、５、５ａ、５ｂ、５ｃ……ディスク駆動装置、６……共通バス、７、７ａ、７ｂ ……ディスク制御装置、８……チャネルパス、９……主システム、１０……副システム、１１……ＬＡＮインタフェース、１２……主記憶、１３……プロセッサ、１４……ＬＡＮネットワーク、１５……共有メモリ、１６……プロセッサ、１７……ローカルメモリ、１８……外部インタフェース、１９……アクセス制御部、２０……バスインタフェース、２１……暗号化プロセッサ、２２、２３……ディレクタ、２４……ワイド・エリア・ネットワーク（ＷＡＮ）、２５……復号化プログラム、２６……暗号化データテーブル、２７……ロジカルユニット番号（ＬＵＮ）、２８……論理ブロックアドレス、２９……書き込みデータ長、３０……書き込みデータ（暗号化）、３１……ロジカルユニット番号（ＬＵＮ）、３２……論理ブロックアドレス、３３……書き込みデータ長、３４……書き込みデータ（平文）、３５……ロジカルユニット番号（ＬＵＮ）、３６……論理ブロックアドレス、３７……書

き込みデータ長、３８……I/0制御プロセッサ、３９……暗号化装置、４０……ログファイル、４１……プロセッサ、４２……ローカルメモリ、４３……ＷＡＮインタフェース、４４……チャネルパスインタフェース、４５……ＷＡＮインタフェース、４６……書き込みデータ長、４７……書き込みデータ（暗号化）。

【書類名】　図面

【図１】

図１


LANネットワーク
14
7b
LAN
インタフェース
11
共有メモリ
暗号化データ
テーブル
15
26
キャッシュ
メモリ
3
6
1b
主記憶
12
LAN
インタフェース
11
25
暗号化
プログラム
プロセッサ
13
I／O制御
プロセッサ
38
8
ホストインタフェース#3
プロセッサ
2d
ディスクインタフェース#1
プロセッサ
4
5
共通バス
8b
ホストインタフェース#2
プロセッサ
2c
ディスクインタフェース#0
プロセッサ
4
5
23
ディレクタ
WAN
24

【図２】

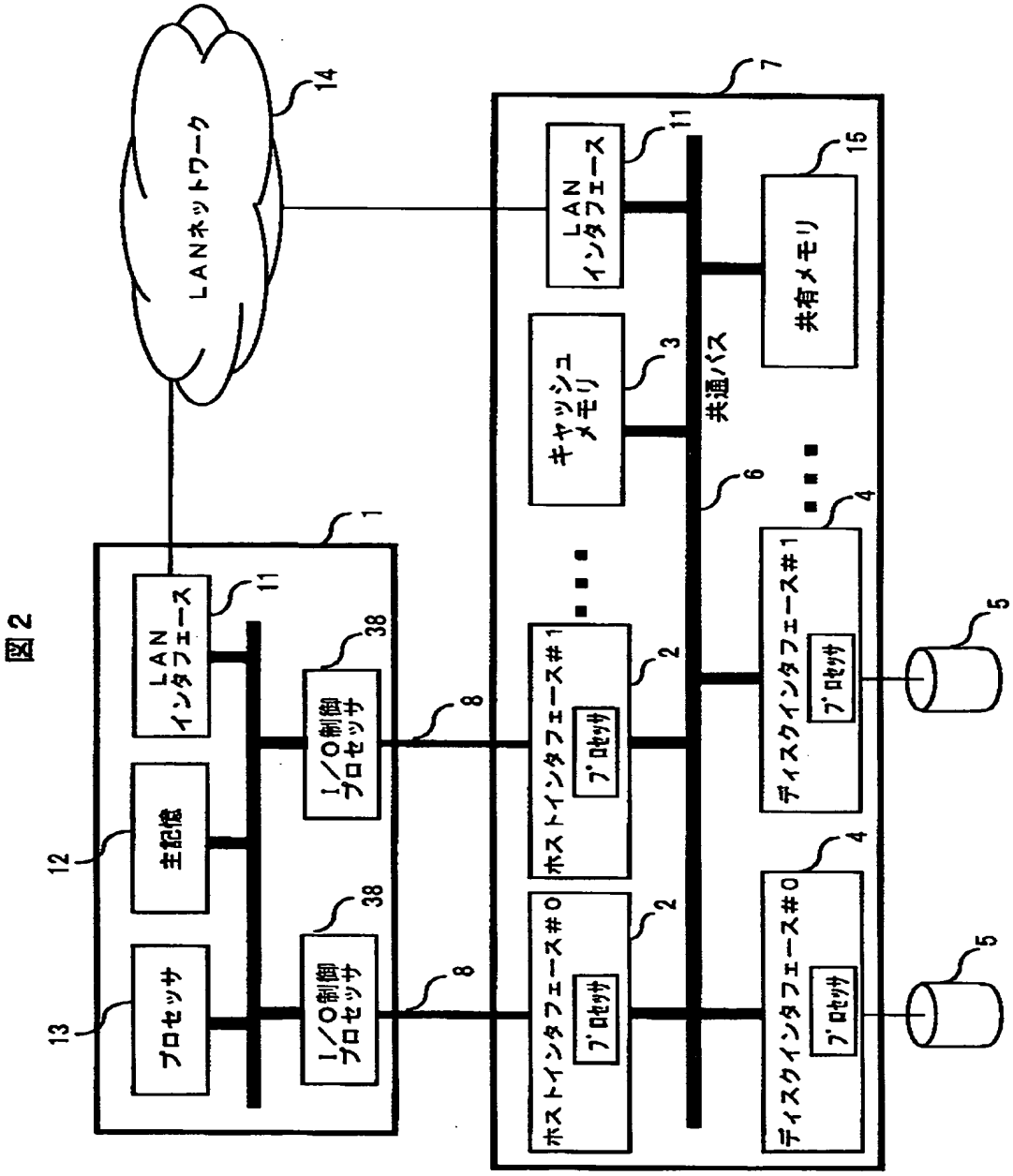

LANネットワーク
14
7
LAN
インタフェース
11
15
共有メモリ
キャッシュ
メモリ
3
共通バス
6
1
LAN
インタフェース
11
38
I/O制御
プロセッサ
8
ホストインタフェース#1
プロセッサ
2
ディスクインタフェース#1
プロセッサ
4
5
12
主記憶
13
プロセッサ
38
I/O制御
プロセッサ
8
ホストインタフェース#0
プロセッサ
2
ディスクインタフェース#0
プロセッサ
4
5

図２

【図３】

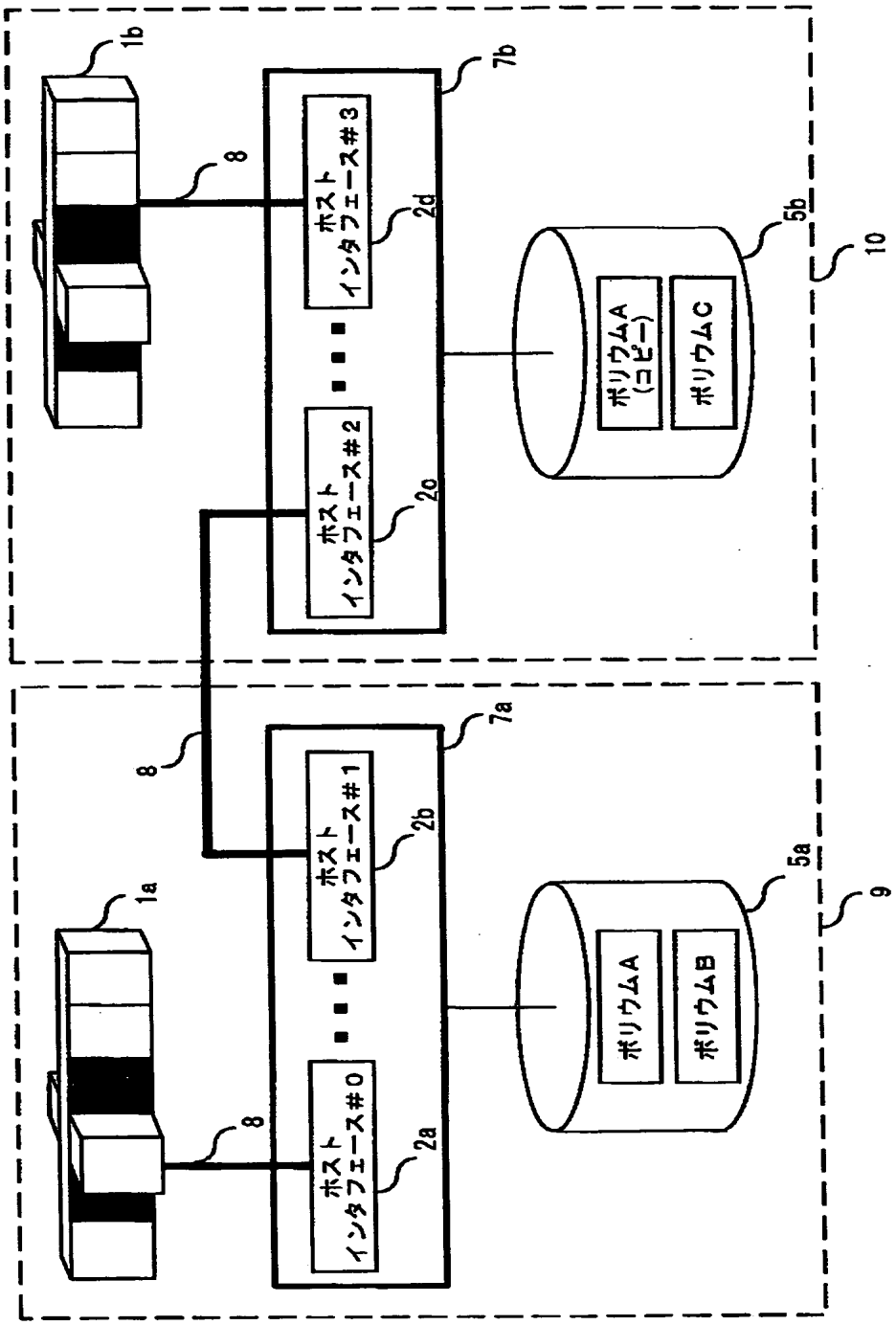
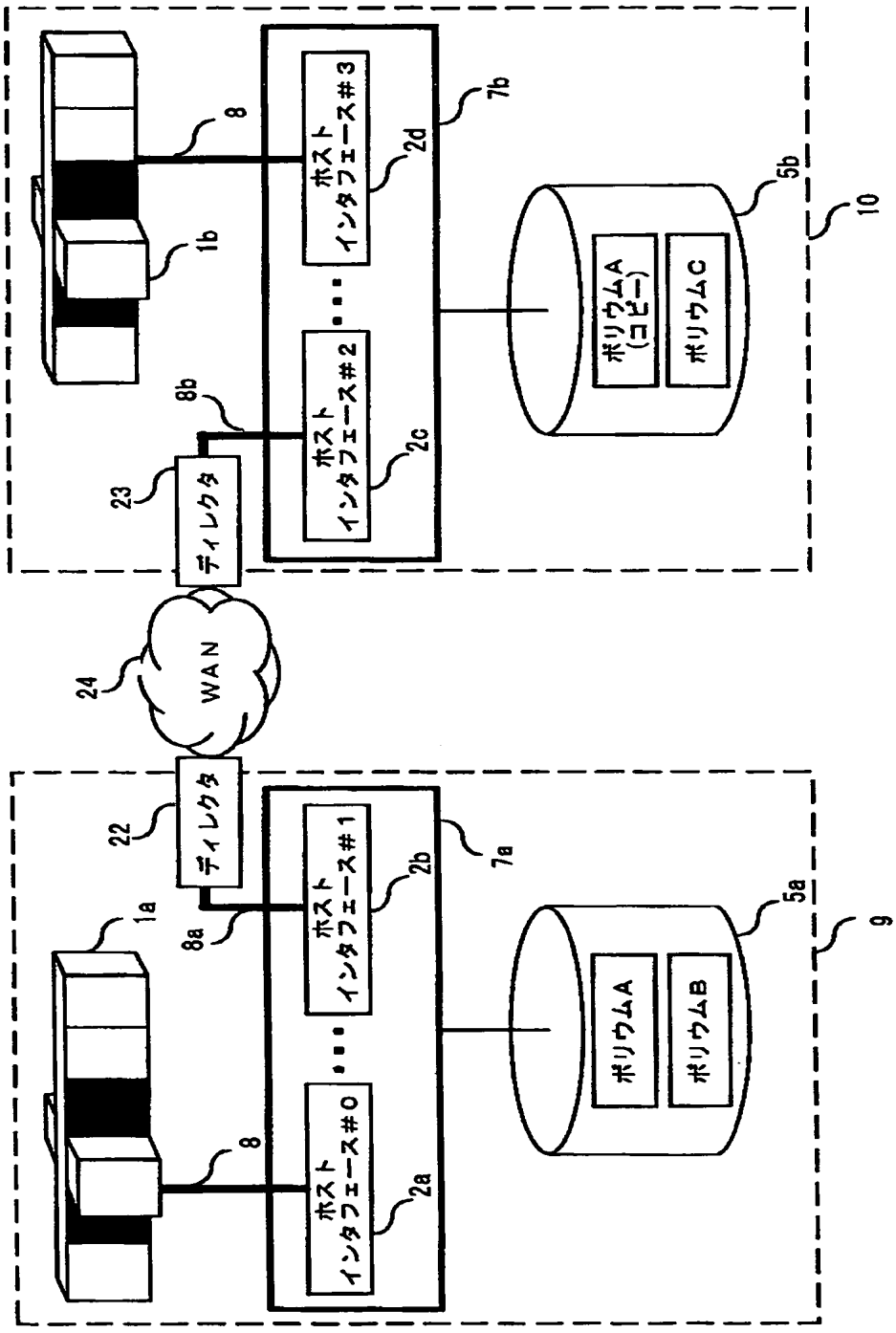

1b
8
7b
ホスト
インタフェース#3
2d
ホスト
インタフェース#2
2c
5b
10
ボリウムA
(コピー)
ボリウムC
8
7a
ホスト
インタフェース#1
2b
1a
5a
9
ボリウムA
ボリウムB
8
ホスト
インタフェース#0
2a

図3

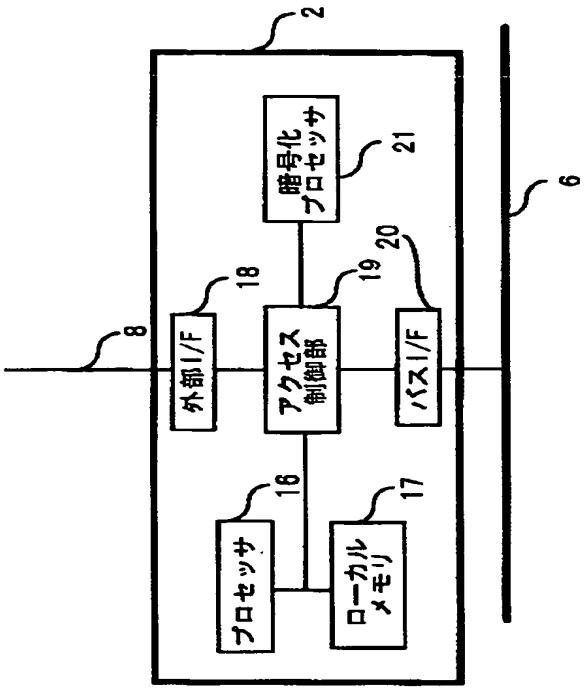
【図４】

図４


10
5b
ボリウムA
(コピー)
ボリウムC
7b
ホスト
インタフェース#3
2d
ホスト
インタフェース#2
2c
8
1b
8b
23
ディレクタ
24
WAN
22
ディレクタ
1a
8a
ホスト
インタフェース#1
2b
7a
ホスト
インタフェース#0
2a
8
5a
9
ボリウムA
ボリウムB

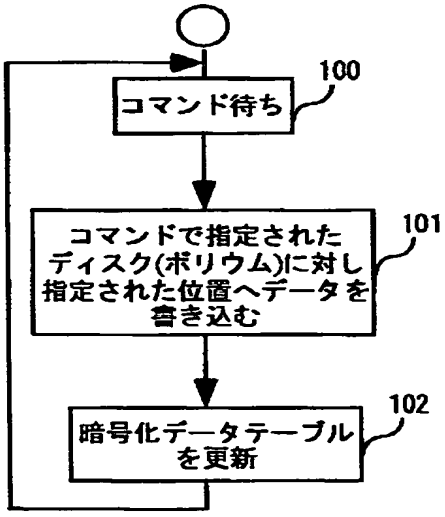
【図５】

図５


2
暗号化プロセッサ
21
6
18
19
20
8
外部I/F
アクセス制御部
バスI/F
16
17
プロセッサ
ローカルメモリ

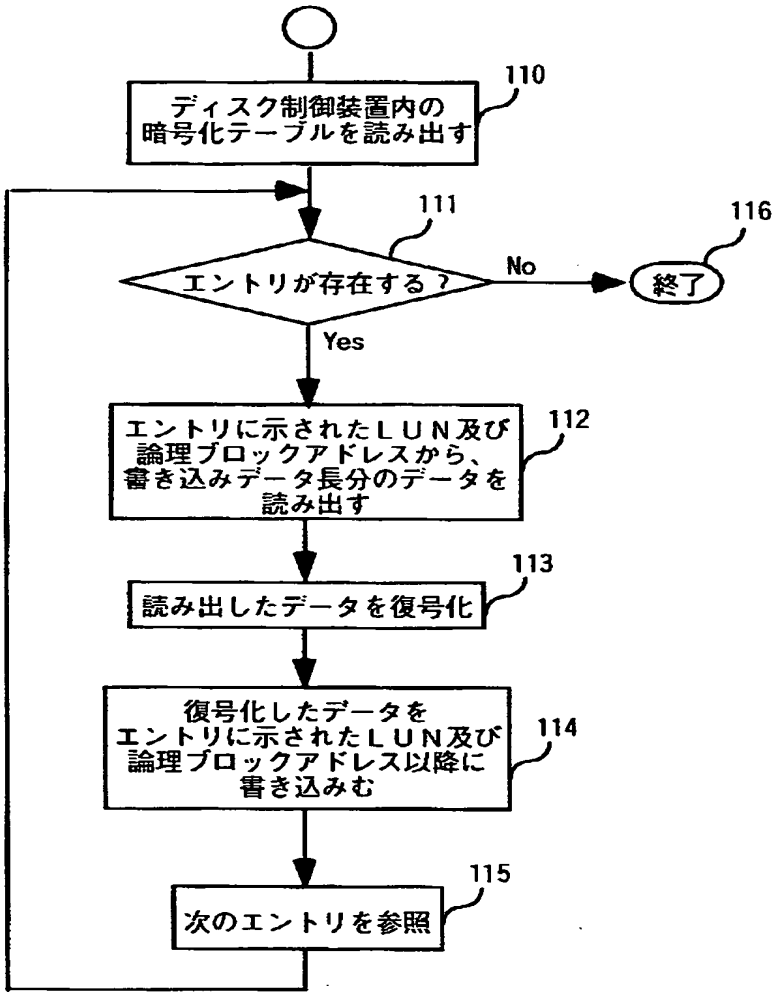
【図６】

図６


100
コマンド待ち
101
コマンドで指定されたディスク(ボリウム)に対し指定された位置へデータを書き込む
102
暗号化データテーブルを更新

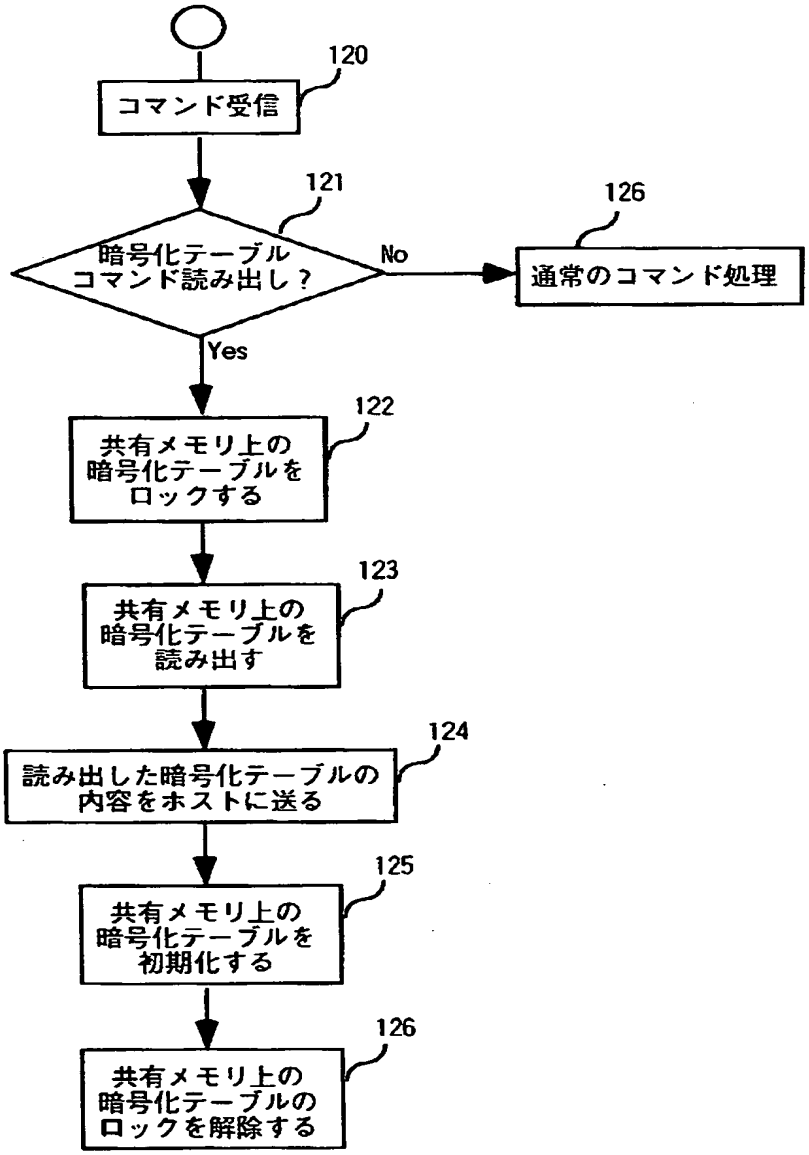
【図７】

図７


ディスク制御装置内の
暗号化テーブルを読み出す
110
111
エントリが存在する？
No
116
終了
Yes
エントリに示されたＬＵＮ及び
論理ブロックアドレスから、
書き込みデータ長分のデータを
読み出す
112
読み出したデータを復号化
113
復号化したデータを
エントリに示されたＬＵＮ及び
論理ブロックアドレス以降に
書き込みむ
114
次のエントリを参照
115

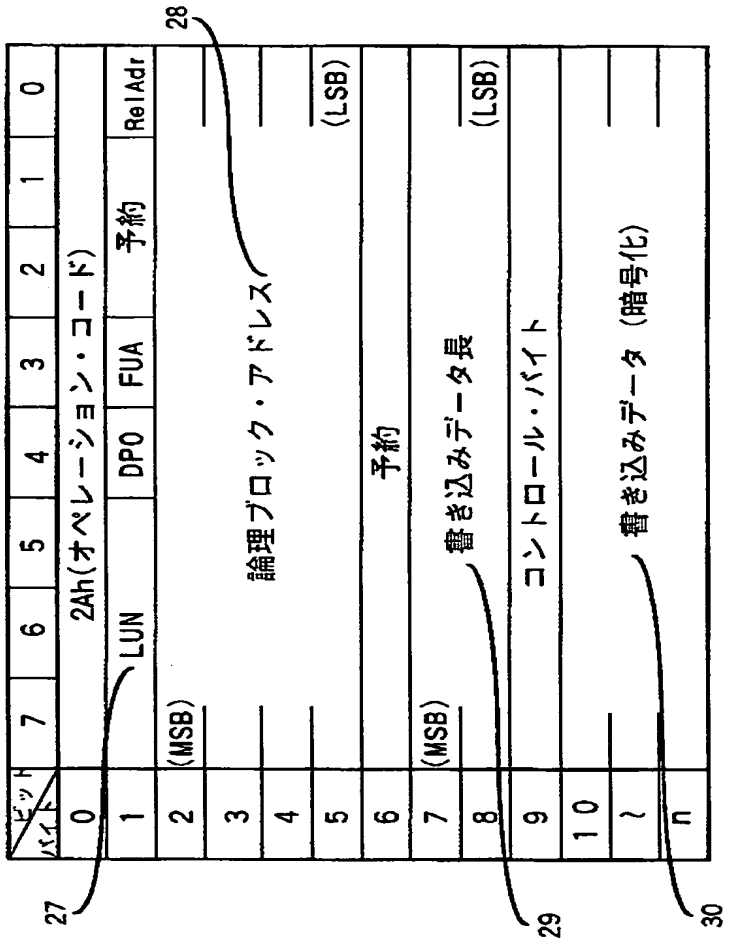
【図８】

図８


120
コマンド受信
121
暗号化テーブル
コマンド読み出し？
No
126
通常のコマンド処理
Yes
122
共有メモリ上の
暗号化テーブルを
ロックする
123
共有メモリ上の
暗号化テーブルを
読み出す
124
読み出した暗号化テーブルの
内容をホストに送る
125
共有メモリ上の
暗号化テーブルを
初期化する
126
共有メモリ上の
暗号化テーブルの
ロックを解除する

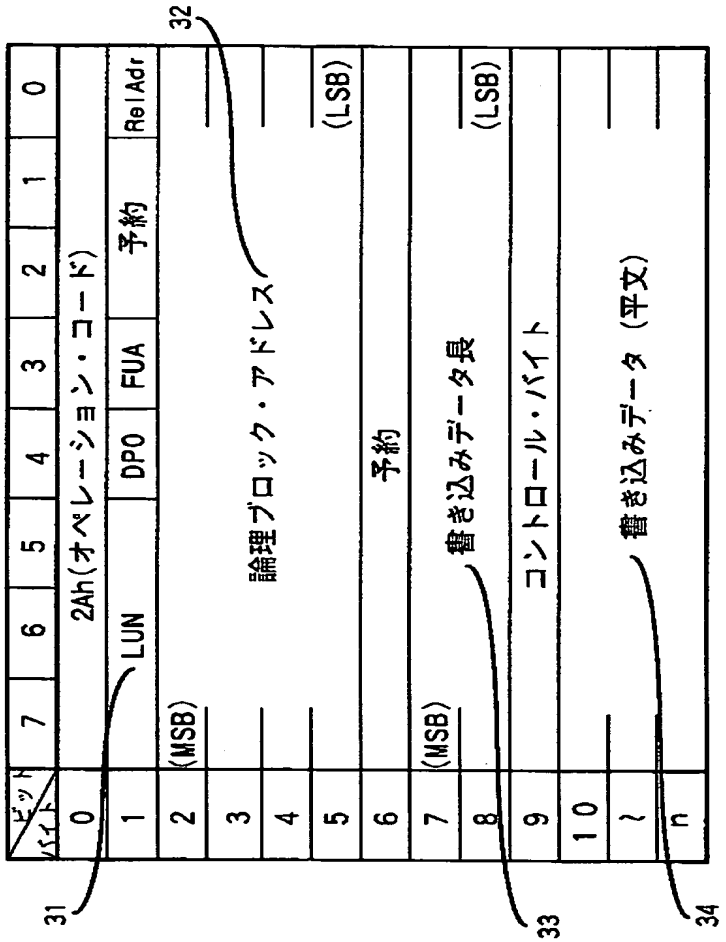
【図９】

図９


ビット
バイト
7
6
5
4
3
2
1
0
0
2Ah(オペレーション・コード)
1
LUN
DPO
FUA
予約
RelAdr
2
(MSB)
論理ブロック・アドレス
3
4
5
(LSB)
6
予約
7
(MSB)
書き込みデータ長
8
(LSB)
9
コントロール・バイト
10
～
n
書き込みデータ（暗号化）
27
28
29
30

【図１０】

図１０


ビット
バイト
7
6
5
4
3
2
1
0
0
1
2
3
4
5
6
7
8
9
10
～
n
2Ahオペレーション・コード
LUN
DPO
FUA
予約
RelAdr
(MSB)
(LSB)
論理ブロック・アドレス
予約
書き込みデータ長
コントロール・バイト
書き込みデータ（平文）
31
32
33
34

【図１１】

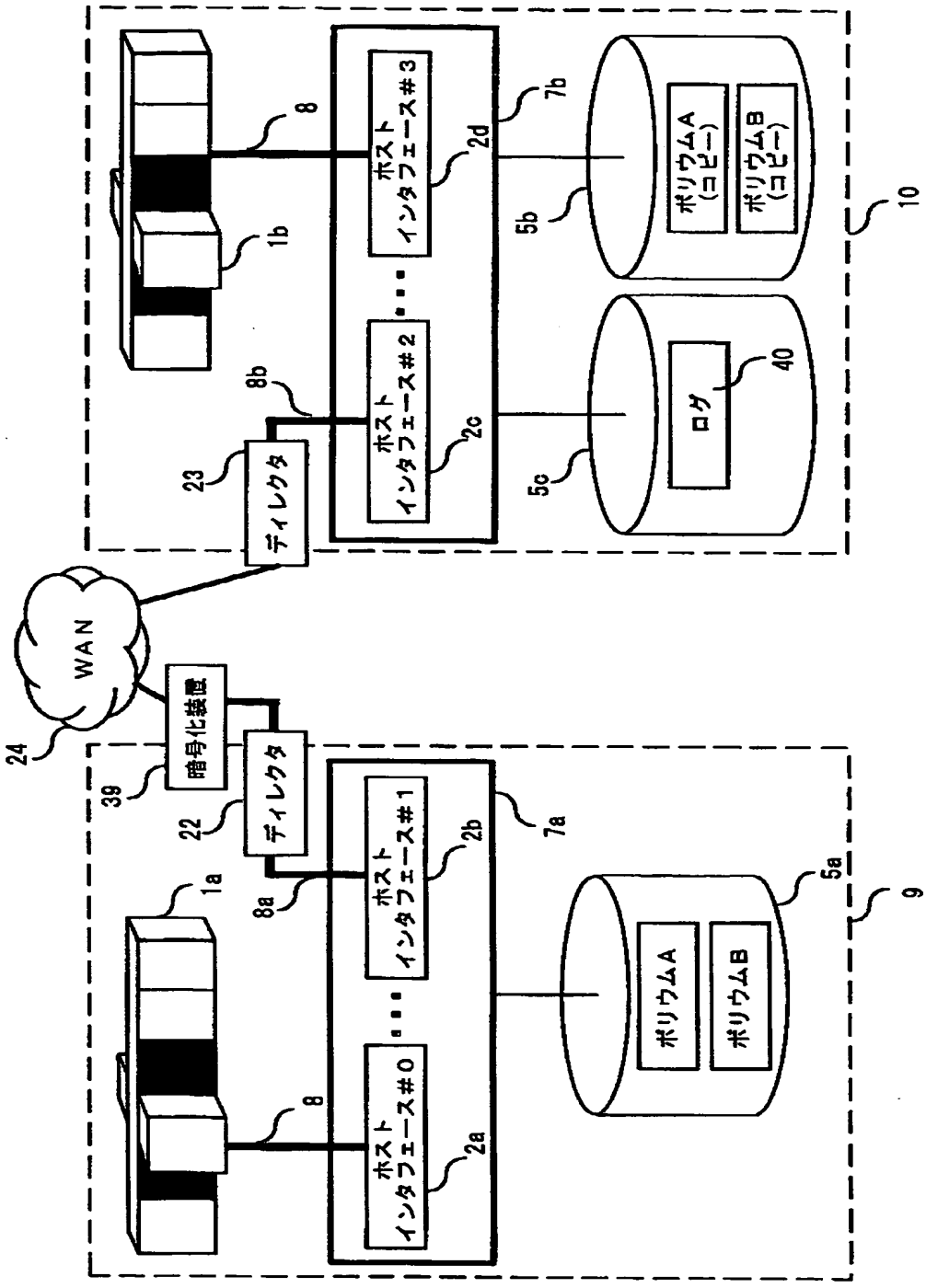
図１１

LUN番号 (35)	論理ブロック・アドレス (36)	書き込みデータ長 (37)
0	１０	１００
5	１２３	７８９
	≀	
1	９４	２０
－1		

出証特２０００－３０８１６８４

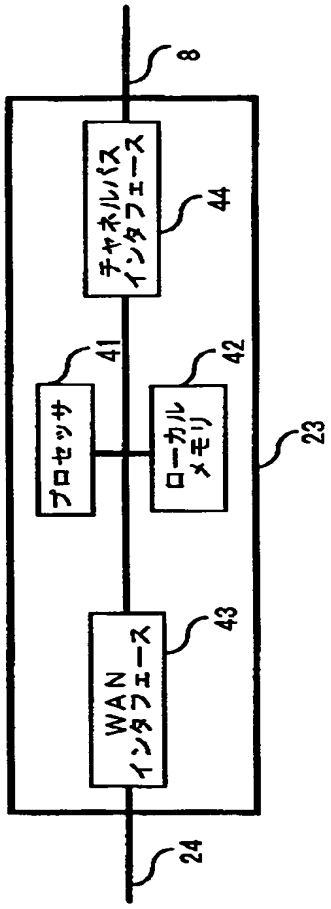
【図１２】

図１２


WAN
24
暗号化装置
39
ディレクタ
22
ディレクタ
23
1a
1b
8
8a
8b
ホスト
インタフェース#0
ホスト
インタフェース#1
ホスト
インタフェース#2
ホスト
インタフェース#3
2a
2b
2c
2d
7a
7b
5a
5b
5c
ボリウムA
ボリウムB
ボリウムA
(コピー)
ボリウムB
(コピー)
ログ
40
9
10

【図１３】

図１３



【図１４】

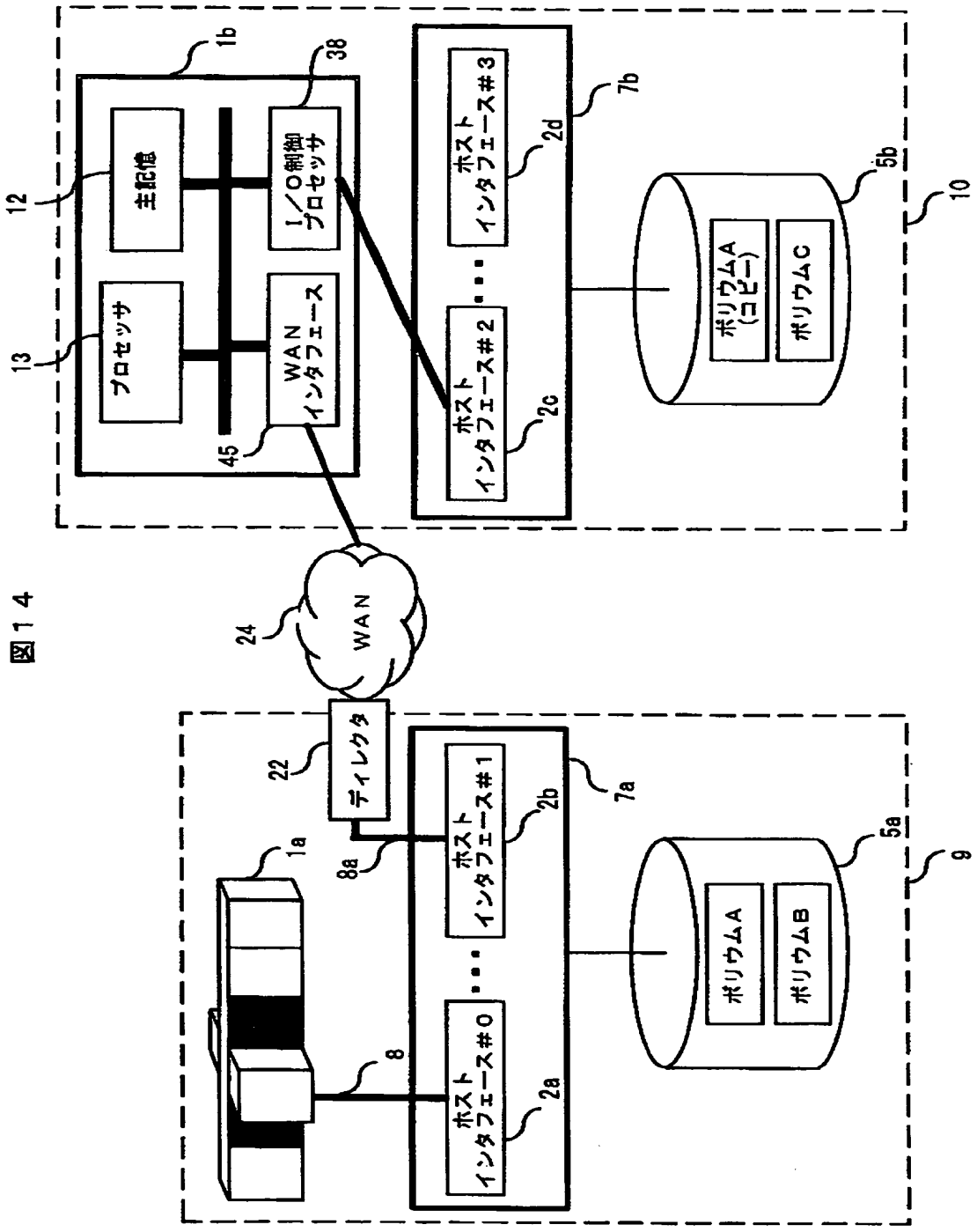

1b
38
12
主記憶
I／O制御プロセッサ
13
プロセッサ
WANインタフェース
45
ホストインタフェース#3
2d
7b
ホストインタフェース#2
2c
5b
10
ボリウムA（コピー）
ボリウムC
24
WAN
22
ディレクタ
1a
8a
ホストインタフェース#1
2b
7a
5a
9
ボリウムA
ボリウムB
8
ホストインタフェース#0
2a

図１４

【図１５】

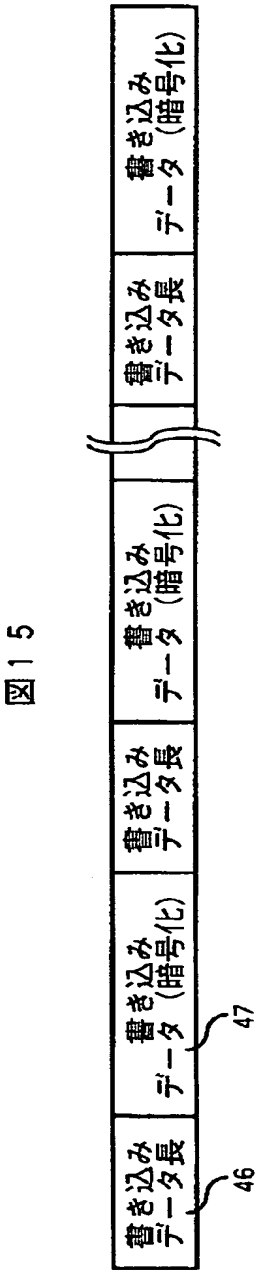

書き込みデータ長
書き込みデータ（暗号化）
47
46
書き込みデータ長
書き込みデータ（暗号化）
書き込みデータ長
書き込みデータ（暗号化）

図１５

【書類名】　要約書

【要約】

【課題】　セキュリティの確保とリモートシステムにおけるスループットの向上を実現する計算機システム及び暗号復号化方法を提供する。

【解決手段】　暗号化データをストレージシステムに書き込む手段、ストレージシステム内のデータが、暗号文か平文かを識別する手段、暗号化データのストレージへの書き込みとは非同期にストレージ内の暗号化データを読み出し復号化し再び書き込む手段を設ける。

【選択図】　図１

出 願 人 履 歴 情 報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所